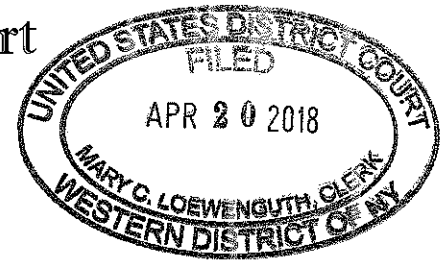


United States District Court
for the
Western District of New York



In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

Email account yzoppolo@hotmail.com, located on computer systems owned, maintained, and/or operated by Microsoft Corporation located at 1065 La Avenida, SVC4/1120, Mountain View, CA 94043, more further described in Attachment A.

Case No. 18-MJ-4045

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property located in the Western District of New York (identify the person or describe the property to be searched and give its location): Email account yzoppolo@hotmail.com, located on computer systems owned, maintained, and/or operated by Microsoft Corporation located at 1065 La Avenida, SVC4/1120, Mountain View, CA 94043, more further described in Attachment A.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized).

See Attachment B, Schedule of Items to be Seized, which attachment is incorporated by reference as if fully set forth herein, all of which are fruits, evidence and instrumentalities of a violation of Title 18, United States Code, Section 1343.

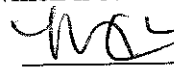
The basis for search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Section 1343.

The application is based on these facts: See attached affidavit.

- ☒ continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Meredith McClatchy, S/A FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: April 20, 2018



Judge's signature

City and state: Rochester, New York

Hon. Marian W. Payson, U.S. Magistrate Judge

Printed name and Title

ATTACHMENT A – MICROSOFT
Property to be Searched

This warrant applies to information associated with the following email accounts stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company located at 1065 La Avenida, SVC4/1120, Mountain View, CA 94043.

- a. vzoppolo@hotmail.com

ATTACHMENT B – MICROSOFT

I. Information to be Seized

The following procedures shall be implemented in executing the warrant:

1. The warrant will be presented to Microsoft, personnel by law enforcement agents. Microsoft, personnel will be directed to isolate those accounts and files described below;
2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts and/or files described below;
3. The Microsoft, system administrator will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;
4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant;
5. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator and will not further review the original duplicate absent an order of the Court.

II. Information to be disclosed by Microsoft

To the extent that the information described in Attachment A is within the possession, custody, or control of Microsoft, Microsoft, is required to disclose the following information to the government for each account or identifier listed in Attachment A:

1. The contents of all emails stored in the account, including copies of emails sent from the account;
2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any creditor bank account number);
3. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

4. All content in the Docs, Calendar, Friend Contacts and Photos areas;
5. Any and all files linked to email accounts of the user; and
6. All records pertaining to communications between Microsoft and any person regarding the account, including contacts with support services and records of actions taken.

III. Information to be seized by the government

1. All records or information, since December 1, 2017, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information, that contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud).
2. The contents of any communications that contain the true identity and or location of individuals who conspired to violate 18 U.S.C. § 1343 (Wire Fraud), including their names and addresses, and any disposition of the proceeds of violations of 18 U.S.C. § 1343 (Wire Fraud).
3. Records relating to who created, or used the account or identifier.
4. Records identifying accounts held with companies providing Internet access or remote storage of tangible items, documents, data, or storage media.
5. Records since December 1, 2017, including, but not limited to, video files, audio files, images, stored messages, recordings, books, documents, and cached web pages, relating to violations of 18 U.S.C. § 1343 (Wire Fraud).
6. Records since December 1, 2017, reflecting communications with or the existence, identity, travel, or whereabouts of, any individuals who conspired to violate 18 U.S.C. § 1343 (Wire Fraud).

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
EMAIL ACCOUNT:

vzoppolo@hotmail.com

Case No. 18-mj-4045

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Meredith McClatchy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since June, 2017. I am currently assigned to the Cyber Squad, Buffalo Division, in Rochester, New York. As part of the Cyber Squad, I work on investigations relating to criminal and national security cyber intrusions. I have gained experience through training and everyday work related to these types of investigations. I am familiar with fundamental operations of the internet, hardware, software, and the communication protocols across each. Experience with similar investigations and working with other FBI Special Agents and computer forensic professionals has expanded my knowledge of internet communications and, more specifically, internet-based obfuscation techniques. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, mobile phones and tablets, and electronically stored information, in conjunction with various criminal investigations.
2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.
3. I make this affidavit in support of an application for a search warrant authorizing the search of an email account controlled by the Service Providers known as Microsoft Corporation (Microsoft), located at 1065 La Avenida, SVC4/1120, Mountain View, CA 94043.
4. The email account and the information to be searched are described in the following paragraphs and in Attachments A and B for the Service Provider. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Service Providers to disclose to the

government records and other information in its possession pertaining to the subscriber or customer associated with the account, including contents of communications.

5. I respectfully submit that probable cause exists to believe that evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1343 (wire fraud), the TARGET OFFENSE, will be found in the account *vzoppolo@hotmail.com*.
6. In my training and experience, I have learned that Microsoft is a company that develops, manufactures, licenses, supports, and sells computer software, consumer electronics, personal computers, and services. Outlook.com is a web-based suite of webmail, contacts, tasks, and calendaring services from Microsoft, and provides free Internet electronic mail (email) access to the public. Hotmail.com was the predecessor to Microsoft's Outlook application, and Hotmail.com email accounts are still operated by Microsoft. I have learned that opened and unopened email for subscribers, may be located on the computers owned or leased by Microsoft. This application for a search warrant seeks authorization solely to search the computer accounts and/or files following the procedures set forth herein.
7. I am familiar with the facts contained in this affidavit based upon my personal involvement in this investigation, information provided by other law enforcement agents, and private companies. Because this affidavit is submitted for the limited purpose of obtaining search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to search the above referenced facilities.

RELEVANT STATUTES

8. This investigation concerns alleged violations of 18 U.S.C. § 1343 –Wire Fraud:
9. 18 U.S.C. § 1343 prohibits a person from devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme.

PROBABLE CAUSE

10. Jones Hospital, located in Wellsville, within the Western District of New York, is an affiliate of the University of Rochester. On December 25, 2017, Jones Hospital was the victim of a Ransomware attack in which an unknown cyber actor inserted malicious code onto the hospital servers which encrypted all their digital records and prevented hospital staff from accessing any electronic data or patient records. The

encryption software contained language which claimed that the cyber actor would provide an encryption key allowing the hospital to recover their digital files upon payment of a ransom.

11. The Ransomware attack was launched from a Jones Hospital server that was exposed to the public internet, herein referred to as the "victim server". The victim server had the IP Address XXX.XXX.174.157.
12. The day after the Ransomware attack, forensic analysis of the victim server was performed by the University of Rochester Information Security Office (ISO). Forensic analysis of the victim server revealed that the cyber actor gained unauthorized access to the victim server using a version of Microsoft's Remote Desktop Protocol (RDP). This software allows a user to remotely access and control a server over a network connection.
13. The cyber actor gained access to the victim server by logging into a specific account, herein referred to as "the account" maintained on the server. The ISO identified this account on the victim server as a test account, which had an easy to guess password. Forensic analysis of the victim server also revealed that the account was accessed without authorization, through RDP, between December 13, 2017 and December 15, 2017.
14. The ISO determined that RDP logs for the account were only available dating back to December 15, 2017. Those logs showed that on December 15, 2017 at 10:19AM EST, the account was successfully logged into from IP Address XXX.XXX.252.255.
15. Further forensic analysis of the account by the ISO revealed that the cyber actor, while logged onto the account, also conducted unrelated web browsing activity on December 13, 2017 and December 14, 2017, as shown by the web logs.
16. Analysis of the web logs from December 13, 2017 revealed that the cyber actor purchased round trip plane tickets using www.tripsta.com, an online booking site. Records identified the flights, date of travel, and passengers for this trip. The flights involved travel between Los Angeles, California and Montevideo, Uruguay.
17. The weblogs for the account also showed that the cyber actor accessed mail.com, then went back to tripsta.com and entered the email address *mariden4@mail.com* to compete the ticket purchase. Your affiant knows that mail.com is a free email service owned by 1&1 Mail & Media, Inc (1&1).
18. One of the passengers entered for the captioned flight purchase was an individual with the initials V.Z. Records checks conducted by FBI Buffalo revealed that V.Z. was from Uruguay and based out of Los Angeles, CA. United States Government record checks

confirmed that V.Z. traveled on the flight from Los Angeles, CA to Montevideo, Uruguay purchased for her by the actor on the victim server.

19. Forensic analysis of the account's web logs from December 13, 2017 also revealed that the cyber actor purchased a Whitepages Premium account. Your affiant knows that Whitepages is an online directory service containing contact information and public records for over 500 million people. Whitepages Premium accounts allow users to search for an individual's landline numbers, current address, previous cities of residence, relatives, associates, mobile phone numbers, previous street addresses, and full address history. Forensic analysis of the account's web logs from December 14, 2017 provided that the cyber actor conducted searches on www.whitepages.com for several individuals. Based on my experience investigating cybercrimes, online directory services, such as Whitepages, are used to look up information on victim credit card holders in order to complete fraudulent transactions.
20. 1&1 provided that the IP Address login history for *mariden4@mail.com* was only retained through December 27, 2017. Subpoenaed records for the account *mariden4@mail.com* showed that the account was logged into from IP Address XXX.XXX.252.255 numerous times between December 27, 2017 and January 3, 2018, the same IP Address found in the RDP logs for the account on the victim server.
21. The subpoenaed records for *mariden4@mail.com* also provided a list of "Forwarding Address" and a list of "Aliases", which contained over two hundred other email addresses. A Forwarding Address is an email address that the subscriber manually sets up to forward mail received by the primary account. An Alias is an email account with the exact same subscriber information and which is created on or around the same time as the primary account. 1&1 was the service provider for all of the email addresses in the Forwarding Address and Aliases list. In a statement to your affiant, a legal specialist provided that the email account *mariden4@mail.com*, and all of the accounts in the Forwarding Address and Aliases list, all had the same subscriber information and IP Address login history. 1&1 determined that *pauldiren@mail.com* was the master account for the email accounts, and the additional Forwarding Address and Aliases, to include *mariden4@mail.com*, were added from the master account.
22. Subpoena returns for the Whitepages premium account purchased on December 13, 2017 identified the subscriber of the account by name and email. It was paid for using a CitiBank Mastercard. The email address associated with this account was in the Forwarding Address List for *mariden4@mail.com*. The IP Address access history for the account showed that the IP Address of the victim server, XXX.XXX.174.157 accessed the account multiple times on December 14, 2017. Shortly thereafter, the real owner of the MasterCard used to open the Whitepages account filed a fraud claim with CitiBank alleging that he did not authorize the purchase. The charge was credited back by the bank.

23. Subpoenaed records from 1&1 provided that the user of the email address associated with the above Whitepages account logged in from IP Address XXX.XXX.252.255 numerous times between December 31, 2017 and January 7, 2018, the same IP Address found in the RDP logs for the account on the victim server.
24. On January 1, 2018, V.Z. flew from Uruguay to the United States on a flight operated by American Airlines. Subpoenaed records from American Airlines provided that the purchaser of V.Z.'s ticket utilized a third party credit card and provided the email address *veronizop@mail.com* at the time of ticket purchase. The email address *vzoppolo@hotmail.com* was added to the flight reservation after the ticket was purchased, and American Airlines emailed *vzoppolo@hotmail.com* on December 27, 2017.
25. The email account *veronizop@mail.com* was in the Alias list for *mariden4@mail.com*. Subpoena returns for *veronizop@mail.com* provided that the user of the account logged in from the IP Address XXX.XXX.252.255 numerous times between January 4, 2018 and January 11, 2018, the same IP Address found in the RDP logs for the account on the victim server.
26. The flight from the United States to Uruguay, as referenced above, was purchased in January 2018 from IP Address XX.XXX.227.87. The FBI had previously encountered this IP Address in an unrelated investigation in August of 2017 and it was associated with a Dark Web Marketplace that sold RDP logon credentials to compromised servers.
27. Subpoenaed records from Virgin Australia provided that V.Z. flew from Los Angeles, CA to Bali, Indonesia with a layover in Brisbane, Australia from January 2, 2018 to January 4, 2018. The purchaser of the flight ticket utilized a third party credit card and provided an email address in the alias list for *mariden4@mail.com* at the time of ticket purchase. While V.Z. was in transit from Los Angeles, CA to Brisbane, Australia, the credit card holder's bank contacted Virgin Australia and notified them that the card holder reported the ticket purchase as unauthorized. V.Z. was contacted by a Virgin Australia fraud analyst when she arrived in Brisbane. When asked for her contact information, V.Z. provided the email address *vzoppolo@hotmail.com*.
28. On January 12, 2018, V.Z. flew from Japan to the United States on a flight operated by American Airlines. Subpoenaed records from American Airlines provided that the purchaser of V.Z.'s ticket utilized a third party credit card and provided an email address in the Alias list of *mariden4@mail.com* at the time of ticket purchase. Subpoenaed records from American Airlines showed that the email address *vzoppolo@hotmail.com* was added to the flight reservation after ticket purchase.
29. Your affiant knows that *hotmail.com* is a free email service provided by Microsoft. Subpoenaed records from Microsoft for the account *vzopppolo@hotmail.com* provided

that the subscriber name for the account was V.Z. The IP Address login history showed that V.Z. accessed her email frequently from June 12, 2017 to December 31, 2017, the end of the scope of the subpoena. Specifically, V.Z. accessed her email on December 30, 2017 and December 31, 2017, immediately prior to her flights on January 1, 2018 and January 2, 2018. V.Z. frequently accessed her email account from IP Address XXX.XXX.9.219, which is geographically located in Los Angeles, CA. The IP Address login history also showed that between December 19, 2017 and December 31, 2017, V.Z. accessed her email account from IP Addresses located in Uruguay, which correlates with her travel.

30. Based on my training and experience, and the facts stated above, it is reasonable to believe that the email accounts operated by the master account *pauldiren@mail.com* are operated by the cyber actor who accessed the Jones Hospital server without authorization from December 13, 2017 to December, 15, 2017. Furthermore, it is reasonable to believe that the cyber actor is accessing servers, without authorization, and using their anonymous status while on the servers to purchase airline tickets and other online subscriptions with unauthorized credit card information.
31. As stated in the facts above, V.Z. repeatedly traveled utilizing tickets purchased for her with unauthorized credit card information by the actor who accessed the victim server. In multiple instances in the scheme, the actor provided an email address operated by the master account *pauldiren@mail.com* at the time of ticket purchase and shortly thereafter added V.Z.'s true email address, *vzoppolo@hotmail.com*, to the flight reservation. Your affiant knows that airlines often use email as a medium through which to communicate with customers, as shown by Virgin Australia and American Airlines. Based on prior behavior, it is reasonable to believe that the cyber actor has added the email address *vzoppolo@hotmail.com* to other flight reservations purchased with unauthorized credit card information, and email communications regarding the flight reservations have been sent to *vzoppolo@hotmail.com*.
32. To successfully execute the scheme, communication is required by the actor who accessed the victim server and V.Z. in order to provide details on the upcoming flight reservations. Based on my training and experience, communications between coconspirators can take place over email. As shown in the subpoena returns for the email account *vzoppolo@hotmail.com*, V.Z. conducted email activity on key dates of fraudulent activity associated with this scheme. With the scheme continuing as recent as January 12, 2018, it is reasonable to believe that the V.Z. sent or received communications regarding this scheme on the email account *vzoppolo@hotmail.com*.
33. For the purposes of this Search Warrant, the Affiant has only included facts relevant to establish probable cause for this affidavit.
34. Based on my knowledge and experience, as well as the facts previously stated, there is probable cause to believe that V.Z. is in control of the email account

vzoppolo@hotmail.com, and the email accounts were used in facilitation of the TARGET OFFENSE.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

35. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."
36. I have had training in the investigation of computer-related crimes. Based on my training, and experience, I know the following:
- a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;
 - b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and
 - c. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.
37. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.

38. The ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, Internet Protocol addresses, and other information both in computer data format and in written record format.
39. "Internet Protocol address" or "IP address" is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet Service Providers (ISPs) assign IP addresses to their customers' computers.
40. "Remote Desktop Protocol" (RDP) is a proprietary protocol which allows a user to remotely connect to another computer via a network connection. The user employs RDP client software for this purpose, which the remote computer must run RDP server software to enable the connection. RDP software clients exist for most versions of Microsoft Windows, Linux, Unix, macOS, iOS, Android, and other operating systems. For example, RDP can be used to access one's work computer from home. While connected, the local user is presented with a graphical interface to the remote machine as well as input capability.
41. The "Dark Web" is the World Wide Web content that exists on overlay networks that use the Internet but require specific software, configurations, or authorization to access. The Dark Web forms a small part of the Deep Web, the part of the Web not indexed by web search engines. A "Dark Web Marketplace" is a commercial website on the Dark Web, functioning primarily as a black market, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, and other illicit goods as well as the sale of legal products.

BACKGROUND REGARDING MICROSOFT

42. Microsoft is the service provider for the email address *vzoppolo@hotmail.com*. Based on my training and experience, I have learned the following about Microsoft:
- a. Microsoft is an American multinational technology company headquartered in Redmond, Washington. It develops, manufactures, licenses, supports, and sells computer software, consumer electronics, personal computers, and services. Its best known products are the Microsoft Windows line of operating systems, the Microsoft Office suite, and the Internet Explorer web browser. One aspect of Microsoft's business involves providing subscribers with free, internet-based

email through their Outlook application. Hotmail is the predecessor to Microsoft's Outlook application, and *Hotmail.com* email accounts are still operated by Microsoft.

- b. Microsoft is considered an electronic communications service ("ECS") provider because it provides its users access to electronic communications service as defined in Title 18, United States Code, Section 2510(15). Internet users sign-up for a subscription for these electronic communication services by registering on the Internet with Microsoft. Microsoft requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information. However, Microsoft does not verify the information provided. As part of its services, Microsoft also provides its subscribers with the ability to set up email accounts;
- c. Microsoft maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts;
- d. Subscribers to Microsoft may access their accounts on servers maintained or owned by Microsoft from any computer connected to the Internet located anywhere in the world;
- e. Any email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by the internet service provider. If the message is not deleted by the subscriber, the account is below the storage limit, and the subscriber accesses the account periodically, that message can remain on Microsoft's servers indefinitely;
- f. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Microsoft's servers, and then transmitted to its end destination. Microsoft users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Microsoft server, the email can remain on the system indefinitely. The sender can delete the stored email message, thereby eliminating it from the email box maintained at Microsoft, but that message will remain in the recipient's email box unless the recipient also deletes it or unless the recipient's account has exceeded its storage limitations;
- g. A Microsoft subscriber can store files, including emails and image files, on servers maintained and/or owned by Microsoft; and
- h. Emails and image files stored on a Microsoft server by a subscriber may not necessarily also be located in the subscriber's home computer. The subscriber may store emails and/or other files on the Microsoft server for which there is

insufficient storage space in the subscriber's own computer or which the subscriber does not wish to maintain in his or her own computer. A search of the subscriber's home, business, or laptop computer will therefore not necessarily uncover files the subscriber has stored on the Microsoft servers.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

43. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require the Service Providers to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I in the Attachment B annexed hereto. Because the Service Providers are not aware of the facts of this investigation, their employees are not in a position to search for relevant evidence. In addition, requiring the Service Providers to perform the search would be a burden upon the companies. If all the Service Providers were asked to do was produce all the files associated with the account, an employee can do that easily. Requiring the Service Providers to search the materials to determine what content is relevant would add to their burden. Upon receipt of the information described in Section I in the Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

44. Based on my training and experience, and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that in the email account located on computer systems owned, maintained, and/or operated by Microsoft Corporation located at 1065 La Avenida, SVC4/1120, Mountain View, CA 94043 there exists evidence, contraband, fruits, and instrumentalities of violations of Title 18 U.S.C. § 1343 (Wire Fraud). I therefore respectfully request that the Court issue a search warrant directed to the Service Providers for the email account identified in the Attachment A for information described in the Attachment B.
45. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) and (c)(1)(A). Specifically, the Court is "a district court of the United States ... that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).
46. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

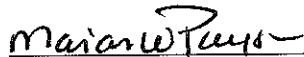
REQUEST FOR SEALING

Because this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto could jeopardize the progress of the investigation. Disclosure of the search warrant at this time could jeopardize the investigation by giving the targets an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.



Meredith McClatchy, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 20 day of April, 2018



HONORABLE MARIAN W. PAYSON
UNITED STATES MAGISTRATE JUDGE